formats
Source DocBook XML
Fichier imprimable PDF
Historique des versions

table des matières
Avant-propos
1. Pourquoi ce guide ?
2. Où trouver ce guide ?
3. Quels sont les systèmes d'exploitation visés ?
1. Sécurisation de base
1.1. Introduction
1.2. Premier conseil : Verrouillez les stations
1.3. Pour Linux
1.4. Pour Windows
1.5. Le lecteur de disquettes
1.6. Le lecteur de CDROM
1.7. N'oubliez pas le mot de passe pour le BIOS
2. La collecte d'informations
2.1. Introduction
2.2. Le Scanner
2.2.1. Qu'est ce qu'un scanner ?
2.2.1.1. Exemple avec Nmap
2.2.2.1. Le scan *vanilla TCP connect*
2.2.2.2. Les scans furtifs
2.2.3. La détermination du système d'exploitation avec Nmap
2.2.5. Comment s'en protéger ?
2.2.6. Documents
2.3. Identifier les versions des logiciels en écoute
2.3.1. Netcat
2.3.1.1. Comment s'en protéger ?
3. Les failles applicatives
3.1. Introduction
3.2. Les installations par défaut
3.3. Les mauvaises configurations
3.4. Les bogues
3.4.1. Des dénis de services applicatifs
3.4.2. Outrepassement de droits
3.4.3. Les scripts
3.5. Les exploits
3.6. Comment s'en proteger ?
4. Les outils indispensables pour la protection
4.1. Introduction
4.2. Le pare-feu *firewall*
4.2.1. La configuration
4.2.2. Les attaques contre les firewalls
4.2.2.1. Avec le *scanner*
4.2.2.2. Comment s'en protéger ?
4.2.2.3. Le firewalking
4.3. Les systèmes de détection d'intrusion (HIDS/NIDS)
4.3.1. Prelude-NIDS
4.3.2. Snort
4.4. Le tunneling
4.4.1. Le protocole AH
4.4.2. Le protocole ESP
4.4.3. Le protocole IPcomp
4.4.4. Le protocole IKE
4.4.5. Les deux modes de fonctionnements de IPsec
4.4.6. Les limitations d'IPsec
4.4.7. Documents
4.5. Nessus
4.5.1. Pour obtenir tout sur Nessus
4.6. User Mode Linux - UML
4.6.1. Documents
5. Surveillance - Dissimulation - Maintien d'accès
5.1. Introduction
5.2. Les chevaux de Troie
5.2.1. Comment s'en protéger ?
5.3. Les backdoors
5.3.1. Les backdoors présentes dans les logiciels.
5.3.1.1. Comment s'en protéger ?
5.3.2. Les backdoors dédiées aux connexions à distance
5.3.2.1. Comment s'en proteger ?
5.4. Les Rootkits
5.4.1. Comment s'en protéger ?
5.5. L'interception des mots de passe en

9.13. Le protocole SMB

Les serveurs SMB sont en écoute sur le port 139 ou 445.

SMB (pour Server Message Block) est le protocole utilisé pour interfacer les partages et les authentifications MICROSOFT. Les clients et serveurs SMB sous Linux et d'autres OS libres utilisent SAMBA pour traiter les échanges avec ce protocole.

SMB possède deux modes d'authentification : le mode "share", dans lequel il associe un mot de passe à une ressource (espace disque, imprimantes ...), et le mode "user", où il associe un mot de passe à un utilisateur. Cet utilisateur peut être aussi propriétaire d'une ressource.

SMB utilise aussi deux modes pour l'envoi de ces mots de passe : encryptés ou non. C'est là que réside toute la faille. C'est le serveur qui donne l'information au client s'il supporte l'encryptage ou non.

Si un pirate parvient à détecter un établisement de session SMB avant cet échange, il peut très bien détourner le flux entre les deux et demander au client d'envoyer son mot de passe en clair et le recevoir.

9.13.1. Les scans de SMB shares

Si vous avez des ressources partagées en accès libre à tout le monde (everyone shares), un pirate utilisera un scanner de share pour les détecter et s'y connecter.

Même si vous protégez ces shares par mot de passe, certains logiciels peuvent tester différents mots de passe en se loguant à la ressource et ainsi tenter différentes combinaisons de mots de passe (voir Chapitre 7, *Sécurisation des mots de passe*).

9.13.2. Comment s'en protéger ?

Pour être sûr que les mots de passe SMB soient envoyés encryptés sur le réseau (même en cas de requêtes «frauduleuses»), vérifiez que la valeur des clés suivantes de la base de registre sont bien égales à 0 :

- Sous Windows NT4 : HKEY\LOCAL\MACHINE\SYSTEM\CurrentControlSet\Services\Rdr\Parameters "EnablePlainTextPasswordi"=dword :00000000";
- Sous Windows XP : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanworkstation\parameters "enableplaintextpassword"=dword :00000000"

Protégez toutes vos ressources par mots de passe, évitez les shares en accès libre à tous le monde et n'oubliez jamais de choisir des mots de passe associés de la bonne façon (voir Chapitre 7, *Sécurisation des mots de passe*).

Ne laissez jamais un serveur SMB en écoute sur Internet, cela est plus que suicidaire. Si vous êtes obligés d'utiliser SMB à travers Internet, utilisez les tunnels (voir Section 4.4, « Le tunneling »).

Sur votre réseau interne, filtrez l'accès sur votre serveur SMB grâce à un firewall.

9.13.3. Document

La description des problèmes de sécurité sur SMB (en anglais) : **SMB/CIFS BY THE ROOT**

réseau.
5.5.1. Comment s'en protéger ?
6. Dispositifs destructeurs
6.1. Introduction
6.2. Le virus
6.2.1. Comment s'en protéger ?
6.3. Les vers
6.3.1. Comment s'en protéger ?
6.4. Les bombes logiques
6.4.1. Comment s'en protéger ?
6.5. Les attaques par déni de services
6.5.1. Le SYN flood
6.5.1.1. Comment s'en protéger ?
6.5.2. L'UDP Flood
6.5.2.1. Comment s'en protéger ?
6.5.3. La fragmentation de paquets
6.5.4. Ping of death
6.5.5. Attaque par réflexion : Smurfing
6.5.5.1. Comment s'en protéger ?
6.5.6. Dénis de services distribués
6.5.7. Bombes e-mail
6.5.7.1. Comment s'en protéger ?
7. Sécurisation des mots de passe
7.1. Introduction
7.2. L'attaque par dictionnaire
7.3. Le brute forcing
7.4. Tester la fiabilité de vos mots de passe !
7.5. Choisir le bon mot de passe
7.6. Prévenir l'utilisateur
8. La base des attaques réseaux
8.1. Introduction
8.2. Détournement de flux
8.2.1. ARP-Poisoning
8.2.1.1. Comment s'en protéger ?
8.2.1.2. Documents
8.2.2. Désynchronisation TCP
8.3. *Man In the Middle* - MITM
8.3.1. Document
8.4. Encapsulation d'IP dans d'autres protocoles.
9. Description d'attaques sur différents protocoles
9.1. Introduction
9.2. Dynamic Host Configuration Protocol - DHCP
9.2.1. Attaque par épuisement de ressources
9.2.2. Faux serveurs DHCP
9.2.3. Comment s'en protéger ?
9.2.4. Documents
9.3. Domain Name Service - DNS
9.3.1. Le DNS ID spoofing
9.3.2. Le DNS cache poisoning
9.3.3. Comment s'en protéger ?
9.3.4. Documents
9.4. FINGER
9.4.1. Comment s'en proteger ?
9.5. FTP
9.5.1. Le serveur FTP anonyme
9.5.1.1. Boucing attack - Attaque par rebonds
9.5.2. Comment s'en protéger ?
9.6. HTTP
9.6.1. Les serveurs trop bavards
9.6.2. Vulnérabilités liées aux applications web
9.6.3. Comment se protéger ?
9.7. IDENT
9.7.1. Comment s'en protéger ?
9.8. IP et l'IP-Spoofing
9.8.1. Un peu de théorie ...
9.8.2. Prévenir l'IP spoofing grâce à Nmap
9.8.3. Comment s'en protéger ?
9.8.4. Document
9.9. NETBIOS
9.9.1. Comment s'en protéger ?
9.9.2. Document
9.10. Network File System - NFS
9.10.1. Les attaques
9.10.2. Comment s'en protéger ?
9.11. Network Information Service - NIS
9.11.1. Les attaques
9.11.2. Comment s'en protéger ?
9.12. PORTMAP
9.12.1. Comment s'en protéger ?
9.13. Le protocole SMB
9.13.1. Les scans de SMB shares
9.13.2. Comment s'en protéger ?
9.13.3. Document
9.14. Le service de messagerie - SMTP
9.14.1. Comment s'en protéger ?
9.15. SQL
9.15.1. L'injection SQL ou *SQL-Injection*
9.15.2. Comment s'en protéger ?
9.15.3. Document
9.16. SSH
9.17. TELNET
9.17.1. Comment s'en protéger ?
9.18. XWINDOW

9.18.1. Les attaques
9.18.2. Comment s'en proteger ?
9.19. Peer To Peer (eDonkey, Kazaa, etc.)
9.19.1. Les outils Peer To Peer sont des vecteurs de virus
9.19.2. Comment s'en protèger ?
10. Sécurité avancée
10.1. Introduction
10.2. L'architecture sécurisée
10.2.1. Le réseau de départ
10.2.2. Le premier niveau de sécurité
10.2.3. Le deuxième niveau de sécurisation
10.2.4. Les niveaux plus élevés
10.3. Développez vos propres utilitaires sécurité
10.3.1. Le programme
10.3.2. Documents
A. Annexes
A.1. Les sites et revues à consulter régulierement
A.2. Remerciements

Dépôt GitHub du site